# Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)

Ministerium: Ministeriet for Samfundssikkerhed og Beredskab

Journalnummer: Ministeriet for Samfundssikkerhed og Beredskab, j.nr. 2025-77

# Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)[1)]

VI FREDERIK DEN TIENDE, af Guds Nåde Danmarks Konge, gør vitterligt:

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

## Kapitel 1

*Anvendelsesområde, jurisdiktion, definitioner m.v.*

**§ 1.** Loven finder anvendelse på offentlige og private enheder, der er omfattet af lovens bilag 1 og 2, jf. dog stk. 2-5 og 7.

*Stk. 2.* Loven finder ikke anvendelse på enheder, i det omfang de er omfattet af lov om styrket beredskab i energisektoren. Loven finder ikke anvendelse på enheder, i det omfang de er omfattet af lov om sikkerhed og beredskab i telesektoren, jf. dog § 1, stk. 2, i denne lov. Loven finder endvidere ikke anvendelse på enheder, der er udpeget i medfør af § 333, stk. 1, i lov om finansiel virksomhed.

*Stk. 3.* Loven finder ikke anvendelse på enheder, hvor sektorspecifikke EU-retsakter og eventuel national gennemførelse heraf har mindst samme virkning som bestemmelserne i §§ 6, 12, 13 og 15.

*Stk. 4.* Loven finder ikke anvendelse på offentlige forvaltningsenheder, som udfører deres aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

*Stk. 5.* Vedkommende minister kan inden for sit område træffe afgørelse om at undtage specifikke enheder, såfremt enhederne udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller udelukkende leverer tjenester til offentlige forvaltningsenheder, der udfører disse aktiviteter, fra forpligtelserne i §§ 6, 8, 12, 13, 15 og 16, for så vidt angår disse aktiviteter eller tjenester. Udfører enheder udelukkende aktiviteter eller leverer udelukkende tjenester af den type som omhandlet i 1. pkt., kan vedkommende minister endvidere træffe afgørelse om at fritage disse enheder for forpligtelserne i medfør af §§ 9 og 10, jf. dog stk. 6.

*Stk. 6.* Der kan ikke fastsættes regler efter stk. 5, hvor en enhed fungerer som tillidstjenesteudbyder.

*Stk. 7.* Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler om, at loven helt eller delvis også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner.

**§ 2.** Under dansk jurisdiktion hører enheder, der er omfattet af lovens anvendelsesområde, og som er etableret i Danmark, jf. dog stk. 2.

*Stk. 2.* DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af henholdsvis cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, der har deres hovedforretningssted i Danmark, jf. stk. 3, hører under dansk jurisdiktion.

*Stk. 3.* En enhed som nævnt i stk. 2 anses for at have sit hovedforretningssted i Den Europæiske Union i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici overvejende træffes. Kan en sådan medlemsstat ikke fastslås, eller hvis sådanne beslutninger ikke træffes i Den Europæiske Union, anses hovedforretningsstedet for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Kan en sådan medlemsstat ikke fastslås, anses hovedforretningsstedet for at være i den medlemsstat, hvor den pågældende enheds forretningssted med det største antal ansatte i Den Europæiske Union er beliggende.

*Stk. 4.* Er en enhed som nævnt i stk. 2 ikke etableret i Den Europæiske Union, men udbyder tjenester inden for Unionen, herunder i Danmark, skal enheden udpege en repræsentant, der er etableret i en af de medlemsstater i Unionen, hvor enhedens tjenester udbydes. Er repræsentanten etableret i Danmark, hører enheden under dansk jurisdiktion. Er der ikke udpeget en repræsentant efter 1. pkt., anses enheden for at høre under jurisdiktionen i de medlemsstater, hvor tjenesterne udbydes.

**§ 3.** I denne lov forstås ved følgende:

1) Centralt kontaktpunkt: Den myndighed, der udøver forbindelsesfunktionen for at sikre grænseoverskridende samarbejde mellem de danske myndigheder, myndigheder i andre medlemsstater i Den Europæiske Union og Den Europæiske Unions institutioner og for at sikre tværsektorielt samarbejde mellem de nationale kompetente myndigheder.
2) Cloudcomputingtjeneste: En digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og fleksibel pulje af delbare computerressourcer, herunder hvor disse ressourcer er fordelt mellem flere lokaliteter.
3) Cybersikkerhed: De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.
4) Cybertrussel: Enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer.
5) Datacentertjeneste: En tjeneste, der omfatter strukturer eller grupper af strukturer, som er beregnet til central opbevaring, sammenkobling og drift af it- og netværksudstyr, der leverer datalagrings-, databehandlings- og datatransporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol.
6) Digital tjeneste: Enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.
7) DNS-tjenesteudbyder: En enhed, der leverer
   a) offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere eller
   b) autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere.
8) Domænenavnesystem (DNS): Et hierarkisk distribueret navngivningssystem, der gør det muligt at identificere internettjenester og -ressourcer, således at slutbrugerudstyr kan benytte internetrouting- og konnektivitetstjenester til at nå disse tjenester og ressourcer.
9) Enhed: En fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser.
10) Enhed, der leverer domænenavnsregistreringstjenester: En registrator eller en agent, der handler på vegne af registratorer, såsom en udbyder eller videresælger af privatlivs- eller proxyregistreringstjenester.
11) Forskningsorganisation: En enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål. Dette indbefatter ikke uddannelsesinstitutioner.
12) Hændelse: En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.
13) Håndtering af hændelser: Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.
14) Ikt-proces: Aktiviteter, der udføres for at udforme, udvikle, levere eller vedligeholde et ikt-produkt eller en ikt-tjeneste.

15) Ikt-produkt: Et element eller en gruppe af elementer i net- og informationssystemer.
16) Ikt-tjeneste: En tjeneste, der helt eller hovedsagelig består af overførsel, lagring, indhentning eller behandling af oplysninger ved hjælp af net- og informationssystemer.
17) Indholdsleveringsnetværk: Et net af geografisk distribuerede servere med det formål at sikre høj tilgængelighed af, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere.
18) Kvalificeret tillidstjeneste: En tillidstjeneste, der opfylder de krav, der er fastsat i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.
19) Kvalificeret tillidstjenesteudbyder: En tillidstjenesteudbyder, der udbyder en eller flere kvalificerede tillidstjenester og har fået tildelt status som kvalificeret tillidstjenesteudbyder af tilsynsorganet i medfør af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.
20) Ledelsesorganet:
    a) For virksomheder omfattet af selskabsloven er ledelsesorganet
        i) bestyrelsen i selskaber, der har en direktion og en bestyrelse,
        ii) direktionen i selskaber, der alene har en direktion, og
        iii) direktionen i selskaber, der både har en direktion og et tilsynsråd.
    b) For virksomheder omfattet af lov om visse erhvervsdrivende virksomheder er ledelsesorganet
        i) bestyrelsen i selskaber, der har en direktion og en bestyrelse,
        ii) direktionen i selskaber, der alene har en direktion, og
        iii) for de selskaber, der hverken har en bestyrelse eller en direktion, det ledelsesorgan, der har en kompetence, der svarer til den almindelige opfattelse af den kompetence, der tilkommer en bestyrelse eller en direktion.
    c) For offentlige myndigheder er ledelsesorganet den øverste administrative ledelse i myndigheden.
21) Net- og informationssystem:
    a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres.
    b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.
    c) Digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
22) Nærvedhændelse: En begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke indtraf.
23) Onlinemarkedsplads: En tjenesteydelse, der gør brug af software, herunder et websted, en del af et websted eller en applikation, der drives af eller på vegne af den erhvervsdrivende, og som giver forbrugere mulighed for at indgå fjernsalgsaftaler med andre erhvervsdrivende eller forbrugere.

24) Onlinesøgemaskine: En digital tjeneste, som giver brugerne mulighed for at indtaste forespørgsler for at foretage søgninger på principielt alle websteder eller alle websteder på et bestemt sprog på grundlag af en forespørgsel om et hvilket som helst emne ved hjælp af et søgeord, en stemmesøgning, en sætning eller andet input, og som fremviser resultater i et hvilket som helst format, hvor der kan findes oplysninger om det ønskede indhold.
25) Platform for sociale netværkstjenester: En platform, der sætter slutbrugere i stand til at komme i forbindelse med hinanden på tværs af forskellige anordninger, navnlig via chats, opslag, videoer og anbefalinger.
26) Repræsentant: En fysisk eller juridisk person, der er etableret i Den Europæiske Union, som udtrykkeligt er udpeget til at handle på vegne af en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester, eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Den Europæiske Union, og som kan kontaktes af en kompetent myndighed eller en Computer Incident Response Team (CSIRT) på enhedens sted, for så vidt angår denne enheds forpligtelser i henhold til NIS 2-direktivet.
27) Risiko: Potentialet for tab eller forstyrrelse som følge af en hændelse, som kommer til udtryk som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer.
28) Sikkerhed i net- og informationssystemer: Net- og informationssystemers evne til på et givent sikkerhedsniveau at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.
29) Sårbarhed: En svaghed, modtagelighed eller fejl ved ikt-produkter eller -tjenester, som kan udnyttes af en cybertrussel.
30) Tillidstjeneste: En elektronisk tjeneste, der normalt udføres mod betaling, og som består af
    a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler eller elektroniske registrerede leveringstjenester og certifikater relateret til tjenester,
    b) generering, kontrol og validering af certifikater for webstedsautentifikation eller
    c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester.
31) Tillidstjenesteudbyder: En fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, enten som en kvalificeret eller ikkekvalificeret tillidstjenesteudbyder.
32) Topdomænenavneadministrator: En enhed, der har fået uddelegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, hvilket inkluderer driften af dets navneservere, vedligeholdelsen af dets databaser og distributionen af topdomænezonefiler til navneservere, uanset om nogen af disse operationer udføres af enheden selv eller outsources, men ikke situationer, hvor topdomænenavne kun anvendes af en administrator til eget brug.
33) Udbyder af administrerede sikkerhedstjenester: En udbyder af administrerede tjenester, der udfører eller yder assistance til aktiviteter vedrørende styring af cybersikkerhedsrisici.
34) Udbyder af administrerede tjenester: En enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af ikt-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand.
35) Væsentlig cybertrussel: En cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en enheds net- og informationssystemer eller på brugerne af enhedens tjenester ved at forårsage betydelig fysisk eller ikkefysisk skade.

*Væsentlige enheder*

**§ 4.** Enheder af en type, som er omfattet af lovens bilag 1, anses for at være væsentlige enheder, hvis enheden opfylder en af følgende betingelser, jf. dog stk. 2 og 3:

1) Enheden beskæftiger 250 personer eller derover.
2) Enheden har en årlig omsætning på over 50 mio. euro og en årlig samlet balance på over 43 mio. euro.

*Stk. 2.* Kommuner og regioner anses som væsentlige enheder, såfremt de med et kommercielt formål udfører opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester og opfylder mindst en af følgende betingelser:

1) Enheden beskæftiger 50 personer eller derover.
2) Enheden har en årlig omsætning på over 10 mio. euro og en årlig samlet balance på over 10 mio. euro.

*Stk. 3.* Uanset deres størrelse anses følgende enheder for at være væsentlige enheder:

1) Kvalificerede tillidstjenesteudbydere og topdomæneadministratorer samt DNS-tjenesteudbydere.
2) Offentlige forvaltningsenheder under den centrale forvaltning.
3) Enheder, der er identificeret som kritiske enheder i henhold til CER-loven.
4) Enheder, der er blevet identificeret som operatører af væsentlige tjenester i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS I-direktivet), jf. dog § 5, stk. 2.
5) Øvrige enheder af en type, som er omfattet af lovens bilag 1 eller 2, hvor mindst en af følgende betingelser er opfyldt, jf. dog § 5, stk. 2:
   a) Enheden er den eneste udbyder i Danmark af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.
   b) En forstyrrelse af den tjeneste, som enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden.
   c) En forstyrrelse af den tjeneste, som enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning.
   d) Enheden er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i Danmark.

*Stk. 4.* Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om, hvornår enheder er omfattet af stk. 3, nr. 5.

*Vigtige enheder*

**§ 5.** Enheder af en type, som er omfattet af lovens bilag 1 eller 2, anses for at være vigtige enheder, hvis enheden ikke opfylder kriterierne for at være væsentlige enheder i medfør af § 4 og enheden opfylder mindst en af følgende betingelser:

1) Enheden beskæftiger 50 personer eller derover.
2) Enheden har en årlig omsætning på over 10 mio. euro og en årlig samlet balance på over 10 mio. euro.

*Stk. 2.* Den kompetente myndighed kan træffe afgørelse om, at en enhed uanset størrelse, som er omfattet af § 4, stk. 3, nr. 4 eller 5, skal anses for at være en vigtig enhed.

*Stk. 3.* Uanset stk. 1, nr. 1 og 2, anses tillidstjenesteudbydere, der ikke opfylder kriterierne for at være væsentlige enheder, for at være vigtige enheder.

## Kapitel 2

*Foranstaltninger til styring af cybersikkerhedsrisici*

**§ 6.** Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte følgende:

1) Politikker for risikoanalyse og informationssystemsikkerhed.
2) Håndtering af hændelser.
3) Driftskontinuitet, herunder backupstyring og reetablering efter en katastrofe og krisestyring.
4) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.
5) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.
6) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.
7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.
8) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.
9) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.
10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

*Stk. 2.* En enhed, der ikke overholder ét eller flere af de krav, der er nævnt i stk. 1, til foranstaltningerne eller regler om krav til foranstaltninger fastsat i medfør af stk. 3, skal uden unødigt ophold træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

*Stk. 3.* Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om foranstaltninger efter stk. 1.

**§ 7.** De foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og 2, og regler fastsat i medfør af § 6, stk. 3, skal være godkendt af enhedens ledelsesorgan. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.

*Stk. 2.* Medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til enhedens øvrige ansatte.

**§ 8.** Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler om, at væsentlige og vigtige enheder skal anvende særlige Ikt-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning, for at påvise overensstemmelse med bestemte krav i § 6, stk. 1, eller regler om foranstaltninger fastsat i medfør af § 6, stk. 3. Produktet kan udvikles af den væsentlige eller vigtige enhed eller indkøbes fra tredjeparter.

## Kapitel 3

*Registrerings- og underretningspligter*

**§ 9.** DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester skal registrere sig hos den relevante kompetente myndighed og i den forbindelse oplyse følgende:

1) Enhedens navn.
2) Adressen på enhedens hovedforretningssted og dens andre forretningssteder i Den Europæiske Union eller, hvis den ikke er etableret i Unionen, den repræsentant, der er udpeget i henhold til § 2, stk. 4, 1. pkt.
3) Den relevante sektor, delsektor og typen, som enheden udgør, jf. lovens bilag 1 eller 2.
4) Ajourførte kontaktoplysninger, herunder e-mailadresser, ip-intervaller og telefonnumre på enheden og kontaktoplysninger på en eventuel udpeget repræsentant i henhold til § 2, stk. 4.
5) De medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester.

*Stk. 2.* Oplysningerne efter stk. 1 skal indgives, senest 3 måneder efter at enheden omfattes af loven.

*Stk. 3.* I tilfælde af ændringer i de oplysninger, der er afgivet i medfør af stk. 1, skal enheden give den relevante kompetente myndighed underretning herom senest 3 måneder efter datoen for ændringen.

**§ 10.** Væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester, skal registrere sig hos den relevante kompetente myndighed og i den forbindelse oplyse følgende, jf. dog § 9:
1) Enhedens navn.
2) Adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, ip-intervaller og telefonnumre.
3) Den relevante sektor og delsektor, som enheden er omfattet af, jf. lovens bilag 1 eller 2.
4) En liste over de øvrige medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet.

*Stk. 2.* Oplysningerne efter stk. 1 skal indgives, senest 2 uger efter at enheden omfattes af loven.

*Stk. 3.* I tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal enheden give den relevante kompetente myndighed underretning herom senest 2 uger efter datoen for ændringen.

*Database over domænenavnsregistreringsdata*

**§ 11.** Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal føre en særskilt database, der indeholder nøjagtige og fuldstændige domænenavnsregistreringsdata.

*Stk. 2.* Databasen efter stk. 1 skal indeholde oplysninger om følgende:
1) Domænenavnet.
2) Registreringsdatoen.
3) Den registreredes navn, e-mailadresse og telefonnummer.
4) E-mailadresse og telefonnummer på det kontaktpunkt, der administrerer domænenavnet, hvis kontaktpunktet er forskelligt fra den registrerede.

*Stk. 3.* Topdomænenavneadministratorerne og enheder, der leverer domænenavnsregistreringstjenester, skal indføre politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at databaserne indeholder nøjagtige og fuldstændige oplysninger. Politikkerne og procedurerne skal gøres offentligt tilgængelige.

*Stk. 4.* Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal uden unødigt ophold efter registreringen af et domænenavn gøre domænenavnsregistreringsdata, som ikke er personoplysninger, offentligt tilgængelige.

*Stk. 5.* Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal på baggrund af en anmodning og efter en konkret vurdering af nødvendigheden give legitime adgangssøgende adgang til specifikke domænenavnsregistreringsdata, herunder personoplysninger. Anmodninger skal besvares senest inden for 72 timer efter modtagelse af anmodningen. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal indføre og offentliggøre politikker og procedurer for adgangen til data.

*Stk. 6.* Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal samarbejde om overholdelsen af de forpligtelser, der er fastsat i stk. 1-5, med henblik på at undgå dobbeltindsamling af domænenavnsregistreringsdata.

*Stk. 7.* Den kompetente myndighed kan meddele topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, forbud eller påbud for at sikre overholdelsen af kravene efter stk. 1-6 eller regler udstedt i medfør af stk. 8.

*Stk. 8.* Digitaliseringsministeren kan fastsætte nærmere regler om krav til politikker og procedurer efter stk. 3 og 5.

*Underretningspligter*

**§ 12.** Væsentlige og vigtige enheder skal underrette den relevante kompetente myndighed og Computer Security Incident Response Team (CSIRT) om enhver væsentlig hændelse. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

*Stk. 2.* En hændelse anses for at være væsentlig, hvis en af følgende betingelser er opfyldt:

1) Hændelsen har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed.
2) Hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikkefysisk skade.

*Stk. 3.* Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om, hvornår en hændelse kan anses for at være væsentlig.

**§ 13.** Underretning efter § 12, stk. 1, skal bestå af følgende og ske på følgende måde:

1) En tidlig varsling, som skal angive, om den væsentlige hændelse mistænkes at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, sendes uden unødigt ophold, og senest inden for 24 timer efter at enheden har fået kendskab til den væsentlige hændelse.
2) En hændelsesunderretning, som skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, sendes uden unødigt ophold, og under alle omstændigheder inden for 72 timer efter at enheden har fået kendskab til den væsentlige hændelse, jf. dog stk. 2.
3) En foreløbig rapport med relevante statusopdateringer sendes efter anmodning fra CSIRT'en.
4) En endelig rapport sendes senest 1 måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Rapporten skal indeholde følgende:
   a) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning.
   b) Den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen.
   c) Anvendte og igangværende afbødende foranstaltninger.
   d) De eventuelle grænseoverskridende virkninger af hændelsen.
5) Pågår hændelsen fortsat på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den underrettende enhed indsende en statusrapport på det pågældende tidspunkt og en endelig rapport, senest 1 måned efter at hændelsen er håndteret.

*Stk. 2.* Tillidstjenesteudbydere skal i tilfælde af væsentlige hændelser afgive underretningen efter stk. 1, nr. 2, uden unødigt ophold og senest inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.

*Stk. 3.* CSIRT'en sikrer, at den underrettende enhed uden unødigt ophold og inden for 24 timer efter modtagelsen af den tidlige varsling, jf. stk. 1, nr. 1, gives et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse. Efter anmodning fra enheden skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

*Frivillige underretninger*

**§ 14.** Offentlige og private enheder kan, uanset at de ikke er omfattet af lovens anvendelsesområde, underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

*Stk. 2.* CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 13. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 13, frem for underretninger efter stk. 1.

*Stk. 3.* Underretninger efter stk. 1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Kapitel 4

*Underretning og oplysning om væsentlige hændelser*

**§ 15.** Væsentlige og vigtige enheder underretter uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt.

*Stk. 2.* Væsentlige og vigtige enheder oplyser uden unødigt ophold modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion herpå. Enhederne skal også informere de pågældende modtagere om den væsentlige cybertrussel, hvor det er relevant.

**§ 16.** Den relevante kompetente myndighed kan efter høring af en enhed, der er ramt af en væsentlig hændelse, informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge videre udbredelse af eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

*Stk. 2.* Den kompetente myndighed kan i de situationer, der er nævnt i stk. 1, træffe afgørelse om, at den relevante enhed informerer offentligheden om den væsentlige hændelse, og bestemme, hvordan denne information skal gives.

*Stk. 3.* CSIRT'en kan efter samme kriterier som i stk. 1 informere offentligheden om væsentlige hændelser, der kan påvirke mere end én sektor.

*Stk. 4.* CSIRT'en kan efter samme kriterier som i stk. 1 informere offentligheden om væsentlige hændelser i andre medlemsstater.

Kapitel 5

*CSIRT'ens opgaver*

**§ 17.** CSIRT'en håndterer it-sikkerhedshændelser og varetager de opgaver, der relaterer sig hertil, herunder følgende opgaver i forhold til væsentlige og vigtige enheder:

1) Efter anmodning fra en væsentlig eller vigtig enhed at yde bistand vedrørende realtids- eller nærrealtidsmonitorering af enhedens net- og informationssystemer.
2) At reagere på hændelser og i den forbindelse yde bistand til de berørte enheder.
3) Efter anmodning fra en væsentlig eller vigtig enhed at foretage en proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning.

*Stk. 2.* Ved udførelsen af opgaver efter stk. 1 kan CSIRT'en prioritere særlige opgaver ud fra en risikobaseret tilgang.

**§ 18.** CSIRT'en sikrer, at fysiske og juridiske personer i anonymiseret form kan rapportere om sårbarheder.

*Stk. 2.* Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om rapportering, håndtering og videregivelse efter stk. 1.

**§ 19.** CSIRT'en faciliterer, at der på frivillig basis kan ske udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber, herunder fællesskaber på europæisk niveau.

*Stk. 2.* Væsentlige og vigtige enheder, der indgår i eller udtræder af cybersikkerhedsfællesskaber efter stk. 1, skal underrette den kompetente myndighed herom.

*Stk. 3.* Offentlige og private enheder kan, uanset at de ikke er omfattet af lovens anvendelsesområde, deltage i den frivillige udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber efter stk. 1.

## Kapitel 6

*Tilsyn og håndhævelse*

**§ 20.** Ministeren for samfundssikkerhed og beredskab fastsætter efter forhandling med vedkommende minister regler om, hvilken myndighed der skal varetage funktionen som kompetent myndighed inden for en given sektor eller delsektor eller for en bestemt type enhed, jf. lovens bilag 1 eller 2. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med den minister, som udnytter bemyndigelsen i § 1, stk. 7, fastsætte regler om, hvilken myndighed der skal varetage funktionen som kompetent myndighed for disse enheder.

*Stk. 2.* For at sikre operationel uafhængighed ved tilsyn med den offentlige forvaltning kan ministeren for samfundssikkerhed og beredskab efter forhandling med en anden minister fastsætte regler om, at tilsyn med Ministeriet for Samfundssikkerhed og Beredskab, herunder underliggende myndigheder, helt eller delvis overlades til den pågældende minister.

*Stk. 3.* Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om koordinering, ansvar, fordeling af opgaver og udveksling af oplysninger mellem henholdsvis de kompetente myndigheder og de kompetente myndigheder og CSIRT'en, herunder i forhold til hændelsesunderretninger efter kapitel 3 og tilsyn samt håndhævelse efter dette kapitel.

*Tilsyns- og kontrolforanstaltninger for væsentlige enheder*

**§ 21.** De kompetente myndigheder fører på deres respektive områder tilsyn med væsentlige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i sit tilsyn anvende følgende tilsynsforanstaltninger over for en væsentlig enhed:

1) Uden retskendelse og mod behørig legitimation foretage kontrol på stedet og eksternt tilsyn, herunder stikprøvekontroller.
2) Foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at enheden får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for den kompetente myndighed.
3) Foretage sikkerhedsaudits.
4) Foretage sikkerhedsscanninger.
5) Kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført.
6) Kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.
7) Kræve at få udleveret dokumentation for gennemførelsen af cybersikkerhedspolitikker.

*Stk. 2.* Ved anvendelsen af tiltagene i stk. 1, nr. 5-7, skal den kompetente myndighed angive formålet hermed og præcisere, hvilke oplysninger der kræves udleveret, og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 5-7, skal udleveres.

*Håndhævelsesforanstaltninger for væsentlige enheder*

**§ 22.** Den kompetente myndighed kan anvende følgende håndhævelsesforanstaltninger over for en væsentlig enhed:

1) Udstede advarsler om enhedens overtrædelse af denne lov.
2) Udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, og frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse, eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.
3) Påbyde enheden at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.
4) Meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
5) Påbyde enheden at underrette de fysiske eller juridiske personer, til hvilke enheden leverer tjenester, eller for hvilke den udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter og om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.
6) Påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.
7) Udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13 og 15 og § 16, stk. 2, og regler udstedt i medfør heraf.
8) Påbyde enheden i ikkeanonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 og resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

**§ 23.** Har en eller flere af de håndhævelsesforanstaltninger, der er pålagt i medfør af § 22, nr. 1-4, vist sig at være utilstrækkelige, kan den kompetente myndighed fastsætte en frist, inden for hvilken den væsentlige enhed skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om følgende, jf. dog stk. 4:

1) Midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, som enheden leverer, eller aktiviteter, der udføres af enheden.
2) Midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed.

*Stk. 2.* Suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil enheden træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

*Stk. 3.* En afgørelse efter stk. 1 kan ikke indbringes for anden administrativ myndighed, men kan af den enhed eller den fysiske person, som afgørelsen vedrører, forlanges indbragt for domstolene.

*Stk. 4.* Bestemmelserne i stk. 1-3 finder ikke anvendelse på offentlige forvaltningsenheder.

*Stk. 5.* Vedkommende minister fastsætter efter forhandling med ministeren for samfundssikkerhed og beredskab regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

*Tilsyns- og kontrolforanstaltninger for vigtige enheder*

**§ 24.** De kompetente myndigheder fører reaktivt tilsyn med vigtige enheders overholdelse af denne lov og regler udstedt i medfør af loven. En kompetent myndighed kan som led i dette tilsyn efter indikationer på, at en vigtig enhed ikke overholder eller ikke har overholdt denne lov eller regler udstedt i medfør af loven, anvende følgende tilsynsforanstaltninger:

1) Uden retskendelse og mod behørig legitimation foretage kontrol på stedet og efterfølgende eksternt tilsyn.
2) Foretage målrettede sikkerhedsaudits eller stille krav om, at enheden får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for den kompetente myndighed.
3) Foretage sikkerhedsscanninger.
4) Kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført.
5) Kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.
6) Kræve at få udleveret dokumentation for gennemførelsen af cybersikkerhedspolitikker.

*Stk. 2.* Ved anvendelse af tiltagene i stk. 1, nr. 4-6, skal den kompetente myndighed angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret, og hvordan og i hvilken form oplysningerne og materialet nævnt i stk. 1, nr. 4-6, skal udleveres.

*Håndhævelsesforanstaltninger over for vigtige enheder*

**§ 25.** En kompetent myndighed kan anvende følgende håndhævelsesforanstaltninger over for en vigtig enhed:

1) Udstede advarsler om enhedens overtrædelse af denne lov.
2) Udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, og frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse, eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.
3) Meddele enheden påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
4) Påbyde enheden at underrette de fysiske eller juridiske personer, til hvilke den leverer tjenester, eller for hvilke den udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter og om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.
5) Påbyde enheden at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.
6) Påbyde enheden i ikkeanonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3 og resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

*Høring af væsentlige og vigtige enheder*

**§ 26.** Inden den kompetente myndighed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 22, 23 eller 25, underrettes den berørte enhed om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Den kompetente myndighed skal give enheden en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde, hvor formålet med foranstaltningen ellers ville forspildes.

## Kapitel 7

*Gensidig bistand*

**§ 27.** Hvor en enhed leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor enheden leverer tjenester i en eller flere medlemsstater og enhedens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet indebærer følgende:

1) De kompetente myndigheder underretter via det centrale kontaktpunkt de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger.
2) De kompetente myndigheder kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger over for enheder i det pågældende land.
3) De kompetente myndigheder yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

*Stk. 2.* De kompetente myndigheder kan efter nærmere aftale gennemføre fælles tilsynstiltag med kompetente myndigheder fra andre medlemsstater i Den Europæiske Union.

*Stk. 3.* Modtages der en anmodning om gensidig bistand, jf. stk. 1, vedrørende DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af henholdsvis cloudcomputingtjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester, kan der træffes passende tilsyns- og håndhævelsesforanstaltninger over for enheden, hvis denne leverer tjenester eller har et net- og informationssystem i Danmark.

## Kapitel 8

*Videregivelse af oplysninger, digital kommunikation, gennemførelsesretsakter og operativ uafhængighed*

**§ 28.** De kompetente myndigheder kan videregive oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union for at varetage de opgaver, som følger af denne lov eller regler udstedt i medfør af denne lov.

**§ 29.** De forpligtelser, der er fastsat i denne lov eller i regler udstedt i medfør af loven, omfatter ikke meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar.

*Stk. 2.* Oplysninger, der modtages eller hidrører fra myndigheder i andre EU-medlemsstater, behandles som fortrolige, såfremt den afgivende myndighed betragter oplysningerne som fortrolige i henhold til EU-regler eller nationale regler.

**§ 30.** Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

**§ 31.** Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur el.lign.

## Kapitel 9

*Straf*

**§ 32.** Med bøde straffes den, der
1) overtræder § 6, stk. 1 eller 2, §§ 9 eller 10, § 11, stk. 1-6, § 12, stk. 1, § 13, stk. 1 eller 2, eller § 15,
2) undlader at efterkomme en kompetent myndigheds afgørelse efter § 23, stk. 1, nr. 1 eller 2,
3) undlader at efterkomme påbud eller forbud efter § 22, stk. 1, nr. 3-6, eller § 25, stk. 1, nr. 3-6,
4) undlader at efterkomme en afgørelse efter § 16, stk. 2, § 21, stk. 1, nr. 2 eller 5-7, eller § 24, stk. 1, nr. 2 eller 4-6, eller
5) hindrer de kompetente myndigheder i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, stk. 1, nr. 1-3.

*Stk. 2.* Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

*Stk. 3.* I forskrifter, der udstedes i medfør af loven, kan der fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

Kapitel 10

*Ikrafttrædelse, overgangsbestemmelser og ændringer i anden lovgivning*

**§ 33.** Loven træder i kraft den 1. juli 2025.

*Stk. 2.* Senest 3 år efter lovens ikrafttræden udarbejder ministeren for samfundssikkerhed og beredskab en rapport om erfaringerne med loven, som oversendes til Folketinget.

*Stk. 3.* Oplysningerne efter § 9, stk. 1, og § 10, stk. 1, skal indgives senest den 1. oktober 2025.

*Stk. 4.* Lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester ophæves.

*Stk. 5.* Lov nr. 437 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. ophæves.

*Stk. 6.* Lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren ophæves.

*Stk. 7.* Lov nr. 441 af 8. maj 2018 om sikkerhed i net- og informationssystemer i transportsektoren ophæves.

Kapitel 11

*Territorialbestemmelse*

**§ 34.** Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning helt eller delvis sættes i kraft for Færøerne og Grønland med de ændringer, som henholdsvis de færøske og de grønlandske forhold tilsiger. Lovens bestemmelser kan sættes i kraft på forskellige tidspunkter.

*Givet på Christiansborg Slot, den 6. maj 2025*

Under Vor Kongelige Hånd og Segl

FREDERIK R.

/ Torsten Schack Pedersen

[1)] Loven gennemfører Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), EU-Tidende 2022, nr. L 333, side 80.

**Bilag 1**

**Sektorer af særlig kritisk betydning**

| *Sektor* | *Delsektor* | *Type enhed* |
|---|---|---|
| 1. Energi | a) Elektricitet | – Elektricitetsvirksomheder som defineret i artikel 2, nr. 57, i Europa-Parlamentets og Rådets direktiv (EU) 2019/944, der varetager »levering« som defineret i nævnte direktivs artikel 2, nr. 12 |
| | | – Distributionssystemoperatører som defineret i artikel 2, nr. 29, i direktiv (EU) 2019/944 |
| | | – Transmissionssystemoperatører som defineret i artikel 2, nr. 35, i direktiv (EU) 2019/944 |
| | | – Producenter som defineret i artikel 2, nr. 38, i direktiv (EU) 2019/944 |
| | | – Udpegede elektricitetsmarkedsoperatører som defineret i artikel 2, nr. 8, i Europa-Parlamentets og Rådets forordning (EU) 2019/943<br>– Markedsdeltagere som defineret i artikel 2, nr. 25, i forordning (EU) 2019/943, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring som defineret i artikel 2, nr. 18, 20 og 59, i direktiv (EU) 2019/944<br>– Operatører af ladestationer, der er ansvarlige for forvaltningen og driften af en ladestation, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne |
| | b) Fjernvarme og fjernkøling | – Operatører af fjernvarme eller fjernkøling som defineret i artikel 2, nr. 19, i Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 |
| | c) Olie | – Olierørledningsoperatører |
| | | – Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission |
| | | – Centrale lagerenheder som defineret i artikel 2, litra f, i Rådets direktiv 2009/119/EF |

| | | |
|---|---|---|
| | d) Gas | – Forsyningsvirksomheder som defineret i artikel 2, nr. 8, i Europa-Parlamentets og Rådets direktiv 2009/73/EF |
| | | – Distributionssystemoperatører som defineret i artikel 2, nr. 6, i direktiv 2009/73/EF |
| | | – Transmissionssystemoperatører som defineret i artikel 2, nr. 4, i direktiv 2009/73/EF |
| | | – Lagersystemoperatører som defineret i artikel 2, nr. 10, i direktiv 2009/73/EF |
| | | – LNG-systemoperatører som defineret i artikel 2, nr. 12, i direktiv 2009/73/EF |
| | | – Naturgasvirksomheder som defineret i artikel 2, nr. 1, i direktiv 2009/73/EF |
| | | – Operatører af naturgasraffinaderier og -behandlingsanlæg |
| | d) Brint | – Operatører inden for brintproduktion, -lagring og -transmission |
| 2) Transport | a) Luft | – Luftfartsselskaber som defineret i artikel 3, nr. 4, i forordning (EF) nr. 300/2008, der anvendes til kommercielle formål |
| | | – Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2, i Europa-Parlamentets og Rådets direktiv 2009/12/EF, lufthavne som defineret i nævnte direktivs artikel 2, nr. 1, herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013; og enheder med tilknyttede anlæg i lufthavne |
| | | – Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som defineret i artikel 2, nr. 1, i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 |
| | b) Jernbane | – Infrastrukturforvaltere som defineret i artikel 3, nr. 2, i Europa-Parlamentets og Rådets direktiv 2012/34/EU |
| | | – Jernbanevirksomheder som defineret i artikel 3, nr. 1, i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i nævnte direktivs artikel 3, nr. 12 |

| | | |
|---|---|---|
| | c) Vand | – Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004, bortset fra de enkelte fartøjer, som drives af disse rederier |
| | | – Driftsorganer i havne som defineret i artikel 3, nr. 1, i Europa-Parlamentets og Rådets direktiv 2005/65/EF, herunder deres havnefaciliteter som defineret i artikel 2, nr. 11, i forordning (EF) nr. 725/2004; og enheder, der opererer anlæg og udstyr i havne |
| | | – Operatører af skibstrafiktjenester som defineret i artikel 3, litra o, i Europa-Parlamentets og Rådets direktiv 2002/59/EF |
| | d) Vejtransport | – Vejmyndigheder som defineret i artikel 2, nr. 12, i Kommissionens delegerede forordning (EU) 2015/962, der er ansvarlige for trafikledelse, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkevæsentlig del af deres generelle aktivitet |
| | | – Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1, i Europa-Parlamentets og Rådets direktiv 2010/40/EU |
| 3. Bankvirksomhed | | – Kreditinstitutter som defineret i artikel 4, nr. 1, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 |
| 4. Finansielle markedsinfrastruktur | | – Operatører af markedspladser som defineret i artikel 4, nr. 24, i Europa-Parlamentets og Rådets direktiv 2014/65/EU |
| | | – Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1, i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 |
| 5. Sundhed | | – Sundhedstjenesteydere som defineret i artikel 3, litra g, i Europa-Parlamentets og Rådets direktiv 2011/24/EU |
| | | – EU-referencelaboratorier, der er omhandlet i artikel 15, i Europa-Parla- |

| | | |
|---|---|---|
| | | mentets og Rådets forordning (EU) 2022/2371 |
| | | – Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som defineret i artikel 1, nr. 2, i Europa-Parlamentets og Rådets direktiv 2001/83/EF<br>– Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE Rev. 2<br>– Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation (»liste over kritisk medicinsk udstyr til folkesundhedsmæssige krisesituationer«) i den i artikel 22 i Europa-Parlamentets og Rådets forordning (EU) 2022/123 anvendte betydning |
| 6. Drikkevand | | – Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1, litra a, i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 bortset fra distributører, for hvilke distribution af drikkevand er en ikkevæsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer |
| 7. Spildevand | | – Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1, 2 og 3, i Rådets direktiv 91/271/EØF, bortset fra virksomheder, for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikkevæsentlig del af deres generelle aktivitet |
| 8. Digital infrastruktur | | – Udbydere af internetudvekslingspunkter |
| | | – DNS-tjenesteudbydere bortset fra operatører af rodnavneservere |
| | | – Topdomænenavneadministratorer |
| | | – Udbydere af cloudcomputingtjenester |
| | | – Udbydere af datacentertjenester |
| | | – Udbydere af indholdsleveringsnetværk |
| | | – Tillidstjenesteudbydere |

| | | |
|---|---|---|
| | | – Udbydere af offentlige elektroniske kommunikationsnet |
| | | – Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester |
| 9. Forvaltning af kt-tjenester (business-to-business) | | – Udbydere af administrerede tjenester<br>– Udbydere af administrerede sikkerhedstjenester |
| 10. Offentlig forvaltning | | – Offentlige forvaltningsenheder under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret |
| | | – Offentlige forvaltningsenheder på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret |
| 11. Rummet | | – Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet |

## Bilag 2

**Andre kritiske sektore**

| *Sektor* | *Delsektor* | *Type enhed* |
|---|---|---|
| 1. Post- og kurertjenester | | – Postbefordrende virksomheder som defineret i artikel 2, nr. 1a, i direktiv 97/67/EF, herunder udbydere af kurertjenester |
| 2. Affaldshåndtering | | – Virksomheder, der varetager affaldshåndtering som defineret i artikel 3, nr. 9, i Europa-Parlamentets og Rådets direktiv 2008/98/EF, bortset fra virksomheder, for hvilke affaldshåndtering ikke er deres vigtigste økonomiske aktivitet |
| 3. Fremstilling, produktion og distribution af kemikalier | | – Virksomheder, der beskæftiger sig med fremstilling af stoffer og distribution af stoffer eller blandinger som omhandlet i artikel 3, nr. 9 og 14, i Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006, og virksomheder, der beskæftiger sig med produktion af artikler som defineret i artikel 3, nr. 3, i nævnte forordning ud af stoffer eller blandinger |
| 4. Produktion, tilvirkning og distribution af fødevarer | | – Fødevarevirksomheder som defineret i artikel 3, nr. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002, der beskæftiger sig med engrosdistribution og industriel produktion og tilvirkning |
| 5. Fremstilling | a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik | – Enheder, der fremstiller medicinsk udstyr som defineret i artikel 2, nr. 1, i Europa-Parlamentets og Rådets forordning (EU) 2017/745, og enheder, der fremstiller medicinsk udstyr til in vitro-diagnostik som defineret i artikel 2, nr. 2, i Europa-Parlamentets og Rådets forordning (EU) 2017/746, med undtagelse af enheder, der fremstiller medicinsk udstyr omhandlet i dette direktivs bilag I, punkt 5, femte led |
| | b) Fremstilling af computere og elektroniske og optiske produkter | – Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 26, i NACE Rev. 2 |

| | | |
|---|---|---|
| | c) Fremstilling af elektrisk udstyr | – Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 27, i NACE Rev. 2 |
| | d) Fremstilling af maskiner og udstyr i.a.n. | – Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 28, i NACE Rev. 2 |
| | e) Fremstilling af motorkøretøjer, påhængsvogne og sættevogne | – Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 29, i NACE Rev. 2 |
| | f) Fremstilling af andre transportmidler | – Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 30, i NACE Rev. 2 |
| 6. Digitale udbydere | | – Udbydere af onlinemarkedspladser |
| | | – Udbydere af onlinesøgemaskiner |
| | | – Udbydere af platforme for sociale netværkstjenester |
| 7. Forskning | | – Forskningsorganisationer |